Amendments to the Claims

1. (currently amended) A system for encrypting and decrypting data formed of a ~~number~~ plurality of bytes using an RC4 stream cipher ~~encryption algorithm~~, comprising:

~~a system bus;~~

[[an]] a hardware-based encryption accelerator ~~arranged~~ configured to execute the RC4 stream cipher ~~encryption algorithm coupled to the system bus~~, the encryption accelerator including a state memory having a plurality of memory locations; and

a system memory coupled to the system bus arranged to store a secret key array associated with the data ,

wherein the hardware-based encryption accelerator is configured to perform an RC4 shuffling operation using portions of the key array, wherein the shuffling operation is performed concurrently with the receipt of each portion of the key array by the encryption accelerator whereby an initial shuffled pattern of substitution values is generated via hardware and stored in the plurality of memory locations.

[[;]] ~~and~~

~~a central processing unit coupled to the system bus, wherein the state memory is initialized via hardware with an incrementing pattern without loading the incrementing pattern from an external memory~~.

2. (canceled)

3. (previously presented) A system as recited in claim 1, further comprising:

a storage unit coupled to the encryption accelerator arranged to store at least a portion of the data to be encrypted.

4-8. (canceled)

9. (original) A system as recited in claim 1, further comprising an external memory coupled to the state memory arranged to store selected state memory values.

10. (original) A system as recited in claim 9, wherein the encryption accelerator is selectively operable in an Initial Mode and a Continuation mode wherein the Initial Mode the system operates in a sequential manner whereas in the continuation mode the state memory is reloaded with the stored state memory values.

11. (currently amended) An encryption accelerator arranged to encrypt and decrypt data formed of a plurality ~~number~~ of bytes using an RC4 stream cipher ~~encryption algorithm~~, comprising:

a combinational logic block arranged to perform a pre-determined logic operation on selected input values;

a state memory array coupled to the combinational logic block arranged to store a plurality of state memory values; and

a state machine coupled to the combinational logic block and the state memory array configured to ~~that directs~~,

initialize ~~initializing~~ via hardware an incrementing pattern of substitution values in the state memory array ~~without loading the incrementing pattern from an external memory~~,

perform a first RC4 ~~performing a~~ shuffling operation using a portion of the key array, wherein the first RC4 shuffling operation is performed concurrently with the receipt of a portion of the key array, ~~on the fly while concurrently retrieving a secret key associated with the data, wherein the shuffling operation includes moving each of the plurality of state memory values based upon the secret key~~,

generate a pseudo-random number as a result of a second RC4 shuffling operation;

byte-wise transfer ~~transferring~~ a portion of the data to the combinational logic block as a first input value,

transfer the generated pseudo-random number ~~transferring a corresponding state memory value~~ to the combinational logic as a second input value,

logically operate ~~operating~~ on the first and second input values by the combinational logic to form a resulting ~~an encrypted~~ data byte, and outputting the ~~encrypted~~ resulting data byte.

12. (cancel)

13. (original) An accelerator as recited in claim 12, wherein the accelerator is coupled to a system memory arranged to store the secret key and wherein the accelerator

is coupled to a CPU in such a way that the accelerator operates to encrypt the data so as to preserve CPU resources.

14. (original) An accelerator as recited in claim 13, where the CPU is coupled to the accelerator and the system memory by way of a system bus.

15. (original) An accelerator as recited in claim 11, further comprising an input latch coupled to the state machine, the state memory array, and the combinational logic block arranged to store the data to be encrypted.

16. (original) An accelerator as recited in claim 11, further comprising an output latch coupled to the state machine, the state memory array, and the combinational logic block arranged to store the encrypted data.

17. (original) An accelerator as recited in claim 11, wherein the logic function is an exclusive OR logic function.

18. (original) An accelerator as recited in claim 14, wherein the data to be encrypted is passed to the input latch by way of the system bus as directed by the CPU.

19. (original) An accelerator as recited in claim 18, wherein the encrypted data is passed to external circuitry as directed by the CPU by way of an output node coupled to the system bus.

20. (original) An accelerator as recited in claim 11, wherein the accelerator further includes a first index counter and a second index counter each of which is connected to and directed by the state machine.

21. (original) An accelerator as recited in claim 11, wherein the accelerator is included in a computing device.

22. (previously presented) An accelerator as recited in claim 21, wherein the computing device is connected to one of the computing devices of the network, wherein the accelerator encrypts a sent message sent to at least one of the network of computing devices and wherein the accelerator decrypts a received message from at least one of the network computing devices.

23. (new) The system of claim 1, wherein the hardware-based encryption accelerator is further configured to generate a pseudorandom number as a result of a second RC4 shuffling.

24. (new) The system of claim 23, wherein the hardware-based encryption accelerator includes a combinational logic block configured to exclusive OR the generated pseudorandom number with a byte of the data.

25. (new) A method for performing an RC4 stream cipher in a hardware-based encryption accelerator, comprising:

(a) initializing a state memory with an incrementing pattern of substitution values;

(b) receiving, at the hardware-based encryption accelerator, a portion of a key array;

(c) shuffling the pattern of substitution values, using an RC4 shuffling operation, concurrently with the receipt of the portion of the key array; and

(d) repeating steps (b) and (c) until each portion of the key array has been received.

26. (new) The method of claim 25, further comprising:

(e) generating a pseudo-random number using a second RC4 shuffling operation.

27. (new) The method of claim 26, further comprising:

(f) exclusively ORing the pseudo-random number with a portion of an input data.

28. (new) The method of claim 27, wherein the input data is plaintext.

29. (new) The method of claim 27, wherein the input data is ciphertext.